The Washington Post
November 6, 2005
The FBI's Secret Scrutiny;
In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans
by Barton Gellman

The FBI came calling in Windsor, Conn., this summer with a document marked for delivery by hand. On Matianuk Avenue, across from the tennis courts, two special agents found their man. They gave George Christian the letter, which warned him to tell no one, ever, what it said.

Under the shield and stars of the FBI crest, the letter directed Christian to surrender "all subscriber information, billing information and access logs of any person" who used a specific computer at a library branch some distance away. Christian, who manages digital records for three dozen Connecticut libraries, said in an affidavit that he configures his system for privacy. But the vendors of the software he operates said their databases can reveal the Web sites that visitors browse, the e-mail accounts they open and the books they borrow.

Christian refused to hand over those records, and his employer, Library Connection Inc., filed suit for the right to protest the FBI demand in public. The Washington Post established their identities -- still under seal in the U.S. Court of Appeals for the 2nd Circuit -- by comparing unsealed portions of the file with public records and information gleaned from people who had no knowledge of the FBI demand.

The Connecticut case affords a rare glimpse of an exponentially growing practice of domestic surveillance under the USA Patriot Act, which marked its fourth anniversary on Oct. 26. "National security letters," created in the 1970s for espionage and terrorism investigations, originated as narrow exceptions in consumer privacy law, enabling the FBI to review in secret the customer records of suspected foreign agents. The Patriot Act, and Bush administration guidelines for its use, transformed those letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies.

The FBI now issues more than 30,000 national security letters a year, according to government sources, a hundredfold increase over historic norms. The letters -- one of which can be used to sweep up the records of many people -- are extending the bureau's reach as never before into the telephone calls, correspondence and financial lives of ordinary Americans.

Issued by FBI field supervisors, national security letters do not need the imprimatur of a prosecutor, grand jury or judge. They receive no review after the fact by the Justice Department or Congress. The executive branch maintains only statistics, which are incomplete and confined to classified reports. The Bush administration defeated legislation and a lawsuit to require a public accounting, and has offered no example in which the use of a national security letter helped disrupt a terrorist plot.

The burgeoning use of national security letters coincides with an unannounced decision to

deposit all the information they yield into government data banks -- and to share those private records widely, in the federal government and beyond. In late 2003, the Bush administration reversed a long-standing policy requiring agents to destroy their files on innocent American citizens, companies and residents when investigations closed. Late last month, President Bush signed Executive Order 13388, expanding access to those files for "state, local and tribal" governments and for "appropriate private sector entities," which are not defined.

National security letters offer a case study of the impact of the Patriot Act outside the spotlight of political debate. Drafted in haste after the Sept. 11, 2001, attacks, the law's 132 pages wrought scores of changes in the landscape of intelligence and law enforcement. Many received far more attention than the amendments to a seemingly pedestrian power to review "transactional records." But few if any other provisions touch as many ordinary Americans without their knowledge.

Senior FBI officials acknowledged in interviews that the proliferation of national security letters results primarily from the bureau's new authority to collect intimate facts about people who are not suspected of any wrongdoing. Criticized for failure to detect the Sept. 11 plot, the bureau now casts a much wider net, using national security letters to generate leads as well as to pursue them. Casual or unwitting contact with a suspect -- a single telephone call, for example -- may attract the attention of investigators and subject a person to scrutiny about which he never learns.

A national security letter cannot be used to authorize eavesdropping or to read the contents of e-mail. But it does permit investigators to trace revealing paths through the private affairs of a modern digital citizen. The records it yields describe where a person makes and spends money, with whom he lives and lived before, how much he gambles, what he buys online, what he pawns and borrows, where he travels, how he invests, what he searches for and reads on the Web, and who telephones or e-mails him at home and at work.

As it wrote the Patriot Act four years ago, Congress bought time and leverage for oversight by placing an expiration date on 16 provisions. The changes involving national security letters were not among them. In fact, as the Dec. 31 deadline approaches and Congress prepares to renew or make permanent the expiring provisions, House and Senate conferees are poised again to amplify the FBI's power to compel the secret surrender of private records.

The House and Senate have voted to make noncompliance with a national security letter a criminal offense. The House would also impose a prison term for breach of secrecy.

Like many Patriot Act provisions, the ones involving national security letters have been debated in largely abstract terms. The Justice Department has offered Congress no concrete information, even in classified form, save for a partial count of the number of letters delivered. The statistics do not cover all forms of national security letters or all U.S. agencies making use of them.

"The beef with the NSLs is that they don't have even a pretense of judicial or impartial scrutiny," said former representative Robert L. Barr Jr. (Ga.), who finds himself allied with the American Civil Liberties Union after a career as prosecutor, CIA analyst and conservative GOP stalwart. "There's no checks and balances whatever on them. It is simply some bureaucrat's decision that they want information, and they can basically just go and get it."

Career investigators and Bush administration officials emphasized, in congressional testimony

and interviews for this story, that national security letters are for hunting terrorists, not fishing through the private lives of the innocent. The distinction is not as clear in practice.

Under the old legal test, the FBI had to have "specific and articulable" reasons to believe the records it gathered in secret belonged to a terrorist or a spy. Now the bureau needs only to certify that the records are "sought for" or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."

That standard enables investigators to look for conspirators by sifting the records of nearly anyone who crosses a suspect's path.

"If you have a list of, say, 20 telephone numbers that have come up . . . on a bad guy's telephone," said Valerie E. Caproni, the FBI's general counsel, "you want to find out who he's in contact with." Investigators will say, " 'Okay, phone company, give us subscriber information and toll records on these 20 telephone numbers,' and that can easily be 100."

Bush administration officials compare national security letters to grand jury subpoenas, which are also based on "relevance" to an inquiry. There are differences. Grand juries tend to have a narrower focus because they investigate past conduct, not the speculative threat of unknown future attacks. Recipients of grand jury subpoenas are generally free to discuss the subpoenas publicly. And there are strict limits on sharing grand jury information with government agencies.

Since the Patriot Act, the FBI has dispersed the authority to sign national security letters to more than five dozen supervisors -- the special agents in charge of field offices, the deputies in New York, Los Angeles and Washington, and a few senior headquarters officials. FBI rules established after the Patriot Act allow the letters to be issued long before a case is judged substantial enough for a "full field investigation." Agents commonly use the letters now in "preliminary investigations" and in the "threat assessments" that precede a decision whether to launch an investigation.

"Congress has given us this tool to obtain basic telephone data, basic banking data, basic credit reports," said Caproni, who is among the officials with signature authority. "The fact that a national security letter is a routine tool used, that doesn't bother me."

If agents had to wait for grounds to suspect a person of ill intent, said Joseph Billy Jr., the FBI's deputy assistant director for counterterrorism, they would already know what they want to find out with a national security letter. "It's all chicken and egg," he said. "We're trying to determine if someone warrants scrutiny or doesn't."

Billy said he understands that "merely being in a government or FBI database . . . gives everybody, you know, neck hair standing up." Innocent Americans, he said, "should take comfort at least knowing that it is done under a great deal of investigative care, oversight, within the parameters of the law."

He added: "That's not going to satisfy a majority of people, but . . . I've had people say, you know, 'Hey, I don't care, I've done nothing to be concerned about. You can have me in your files and that's that.' Some people take that approach."

In Room 7975 of the J. Edgar Hoover Building, around two corners from the director's suite, the chief of the FBI's national security law unit sat down at his keyboard about a month after the Patriot Act became law. Michael J. Woods had helped devise the FBI wish list for surveillance powers. Now he offered a caution.

"NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information," he wrote in a Nov. 28, 2001, "electronic communication" to the FBI's 56 field offices. "However, they must be used judiciously." Standing guidelines, he wrote, "require that the FBI accomplish its investigations through the 'least intrusive' means. . . . The greater availability of NSLs does not mean that they should be used in every case."

Woods, who left government service in 2002, added a practical consideration. Legislators granted the new authority and could as easily take it back. When making that decision, he wrote, "Congress certainly will examine the manner in which the FBI exercised it."

Looking back last month, Woods was struck by how starkly he misjudged the climate. The FBI disregarded his warning, and no one noticed.

"This is not something that should be automatically done because it's easy," he said. "We need to be sure . . . we don't go overboard."

One thing Woods did not anticipate was then-Attorney General John D. Ashcroft's revision of Justice Department guidelines. On May 30, 2002, and Oct. 31, 2003, Ashcroft rewrote the playbooks for investigations of terrorist crimes and national security threats. He gave overriding priority to preventing attacks by any means available.

Ashcroft remained bound by Executive Order 12333, which requires the use of the "least intrusive means" in domestic intelligence investigations. But his new interpretation came close to upending the mandate. Three times in the new guidelines, Ashcroft wrote that the FBI "should consider . . . less intrusive means" but "should not hesitate to use any lawful techniques . . . even if intrusive" when investigators believe them to be more timely. "This point," he added, "is to be particularly observed in investigations relating to terrorist activities."

As the Justice Department prepared congressional testimony this year, FBI headquarters searched for examples that would show how expanded surveillance powers made a difference. Michael Mason, who runs the Washington field office and has the rank of assistant FBI director, found no ready answer.

"I'd love to have a made-for-Hollywood story, but I don't have one," Mason said. "I am not even sure such an example exists."

What national security letters give his agents, Mason said, is speed.

"I have 675 terrorism cases," he said. "Every one of these is a potential threat. And anything I can do to get to the bottom of any one of them more quickly gets me closer to neutralizing a potential threat."

Because recipients are permanently barred from disclosing the letters, outsiders can make no

assessment of their relevance to Mason's task.

Woods, the former FBI lawyer, said secrecy is essential when an investigation begins because "it would defeat the whole purpose" to tip off a suspected terrorist or spy, but national security seldom requires that the secret be kept forever. Even mobster "John Gotti finds out eventually that he was wiretapped" in a criminal probe, said Peter Swire, the federal government's chief privacy counselor until 2001. "Anyone caught up in an NSL investigation never gets notice."

To establish the "relevance" of the information they seek, agents face a test so basic it is hard to come up with a plausible way to fail. A model request for a supervisor's signature, according to internal FBI guidelines, offers this one-sentence suggestion: "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months."

Edward L. Williams, the chief division counsel in Mason's office, said that supervisors, in practice, "aren't afraid to ask . . . 'Why do you want to know?' " He would not say how many requests, if any, are rejected.

Those who favor the new rules maintain -- as Sen. Pat Roberts (R-Kan.), chairman of the Senate Select Committee on Intelligence, put it in a prepared statement -- that "there has not been one substantiated allegation of abuse of these lawful intelligence tools."

What the Bush administration means by abuse is unauthorized use of surveillance data -- for example, to blackmail an enemy or track an estranged spouse. Critics are focused elsewhere. What troubles them is not unofficial abuse but the official and routine intrusion into private lives.

To Jeffrey Breinholt, deputy chief of the Justice Department's counterterrorism section, the civil liberties objections "are eccentric." Data collection on the innocent, he said, does no harm unless "someone [decides] to act on the information, put you on a no-fly list or something." Only a serious error, he said, could lead the government, based on nothing more than someone's bank or phone records, "to freeze your assets or go after you criminally and you suffer consequences that are irreparable." He added: "It's a pretty small chance."

"I don't necessarily want somebody knowing what videos I rent or the fact that I like cartoons," said Mason, the Washington field office chief. But if those records "are never used against a person, if they're never used to put him in jail, or deprive him of a vote, et cetera, then what is the argument?"

Barr, the former congressman, said that "the abuse is in the power itself."

"As a conservative," he said, "I really resent an administration that calls itself conservative taking the position that the burden is on the citizen to show the government has abused power, and otherwise shut up and comply."

At the ACLU, staff attorney Jameel Jaffer spoke of "the profound chilling effect" of this kind of surveillance: "If the government monitors the Web sites that people visit and the books that they read, people will stop visiting disfavored Web sites and stop reading disfavored books. The FBI should not have unchecked authority to keep track of who visits [al-Jazeera's Web site] or who

visits the Web site of the Federalist Society."

Ready access to national security letters allows investigators to employ them routinely for "contact chaining."

"Starting with your bad guy and his telephone number and looking at who he's calling, and [then] who they're calling," the number of people surveilled "goes up exponentially," acknowledged Caproni, the FBI's general counsel.

But Caproni said it would not be rational for the bureau to follow the chain too far. "Everybody's connected" if investigators keep tracing calls "far enough away from your targeted bad guy," she said. "What's the point of that?"

One point is to fill government data banks for another investigative technique. That one is called "link analysis," a practice Caproni would neither confirm nor deny.

Two years ago, Ashcroft rescinded a 1995 guideline directing that information obtained through a national security letter about a U.S. citizen or resident "shall be destroyed by the FBI and not further disseminated" if it proves "not relevant to the purposes for which it was collected." Ashcroft's new order was that "the FBI shall retain" all records it collects and "may disseminate" them freely among federal agencies.

The same order directed the FBI to develop "data mining" technology to probe for hidden links among the people in its growing cache of electronic files. According to an FBI status report, the bureau's office of intelligence began operating in January 2004 a new Investigative Data Warehouse, based on the same Oracle technology used by the CIA. The CIA is generally forbidden to keep such files on Americans.

Data mining intensifies the impact of national security letters, because anyone's personal files can be scrutinized again and again without a fresh need to establish relevance.

"The composite picture of a person which emerges from transactional information is more telling than the direct content of your speech," said Woods, the former FBI lawyer. "That's certainly not been lost on the intelligence community and the FBI."

Ashcroft's new guidelines allowed the FBI for the first time to add to government files consumer data from commercial providers such as LexisNexis and ChoicePoint Inc. Previous attorneys general had decided that such a move would violate the Privacy Act. In many field offices, agents said, they now have access to ChoicePoint in their squad rooms.

What national security letters add to government data banks is information that no commercial service can lawfully possess. Strict privacy laws, for example, govern financial and communications records. National security letters -- along with the more powerful but much less frequently used secret subpoenas from the Foreign Intelligence Surveillance Court -- override them.

The bureau displayed its ambition for data mining in an emergency operation at the end of 2003.

The Department of Homeland Security declared an orange alert on Dec. 21 of that year, in part

because of intelligence that hinted at a New Year's Eve attack in Las Vegas. The identities of the plotters were unknown.

The FBI sent Gurvais Grigg, chief of the bureau's little-known Proactive Data Exploitation Unit, in an audacious effort to assemble a real-time census of every visitor in the nation's most-visited city. An average of about 300,000 tourists a day stayed an average of four days each, presenting Grigg's team with close to a million potential suspects in the ensuing two weeks.

A former stockbroker with a degree in biochemistry, Grigg declined to be interviewed. Government and private sector sources who followed the operation described epic efforts to vacuum up information.

An interagency task force began pulling together the records of every hotel guest, everyone who rented a car or truck, every lease on a storage space, and every airplane passenger who landed in the city. Grigg's unit filtered that population for leads. Any link to the known terrorist universe -- a shared address or utility account, a check deposited, a telephone call -- could give investigators a start.

"It was basically a manhunt, and in circumstances where there is a manhunt, the most effective way of doing that was to scoop up a lot of third party data and compare it to other data we were getting," Breinholt said.

Investigators began with emergency requests for help from the city's sprawling hospitality industry. "A lot of it was done voluntary at first," said Billy, the deputy assistant FBI director.

According to others directly involved, investigators turned to national security letters and grand jury subpoenas when friendly persuasion did not work.

Early in the operation, according to participants, the FBI gathered casino executives and asked for guest lists. The MGM Mirage company, followed by others, balked.

"Some casinos were saying no to consent [and said], 'You have to produce a piece of paper,' " said Jeff Jonas, chief scientist at IBM Entity Analytics, who previously built data management systems for casino surveillance. "They don't just market 'What happens in Vegas stays in Vegas.' They want it to be true."

The operation remained secret for about a week. Then casino sources told Rod Smith, gaming editor of the Las Vegas Review-Journal, that the FBI had served national security letters on them. In an interview for this article, one former casino executive confirmed the use of a national security letter. Details remain elusive. Some law enforcement officials, speaking on the condition of anonymity because they had not been authorized to divulge particulars, said they relied primarily on grand jury subpoenas. One said in an interview that national security letters may eventually have been withdrawn. Agents encouraged voluntary disclosures, he said, by raising the prospect that the FBI would use the letters to gather something more sensitive: the gambling profiles of casino guests. Caproni declined to confirm or deny that account.

What happened in Vegas stayed in federal data banks. Under Ashcroft's revised policy, none of the information has been purged. For every visitor, Breinholt said, "the record of the Las Vegas

hotel room would still exist."

Grigg's operation found no suspect, and the orange alert ended on Jan. 10, 2004."The whole thing washed out," one participant said.

At around the time the FBI found George Christian in Connecticut, agents from the bureau's Charlotte field office paid an urgent call on the chemical engineering department at North Carolina State University in Raleigh. They were looking for information about a former student named Magdy Nashar, then suspected in the July 7 London subway bombing but since cleared of suspicion.

University officials said in interviews late last month that the FBI tried to use a national security letter to demand much more information than the law allows.

David T. Drooz, the university's senior associate counsel, said special authority is required for the surrender of records protected by educational and medical privacy. The FBI's first request, a July 14 grand jury subpoena, did not appear to supply that authority, Drooz said, and the university did not honor it. Referring to notes he took that day, Drooz said Eric Davis, the FBI's top lawyer in Charlotte, "was focused very much on the urgency" and "he even indicated the case was of interest to President Bush."

The next day, July 15, FBI agents arrived with a national security letter. Drooz said it demanded all records of Nashar's admission, housing, emergency contacts, use of health services and extracurricular activities. University lawyers "looked up what law we could on the fly," he said. They discovered that the FBI was demanding files that national security letters have no power to obtain. The statute the FBI cited that day covers only telephone and Internet records.

"We're very eager to comply with the authorities in this regard, but we needed to have what we felt was a legally valid procedure," said Larry A. Neilsen, the university provost.

Soon afterward, the FBI returned with a new subpoena. It was the same as the first one, Drooz said, and the university still had doubts about its legal sufficiency. This time, however, it came from New York and summoned Drooz to appear personally. The tactic was "a bit heavy-handed," Drooz said, "the implication being you're subject to contempt of court." Drooz surrendered the records.

The FBI's Charlotte office referred questions to headquarters. A high-ranking FBI official, who spoke on the condition of anonymity, acknowledged that the field office erred in attempting to use a national security letter. Investigators, he said, "were in a big hurry for obvious reasons" and did not approach the university "in the exact right way."

The electronic docket in the Connecticut case, as the New York Times first reported, briefly titled the lawsuit Library Connection Inc. v. Gonzales. Because identifying details were not supposed to be left in the public file, the court soon replaced the plaintiff's name with "John Doe."

George Christian, Library Connection's executive director, is identified in his affidavit as "John Doe 2." In that sworn statement, he said people often come to libraries for information that is "highly sensitive, embarrassing or personal." He wanted to fight the FBI but feared calling a lawyer because the letter said he could not disclose its existence to "any person." He consulted

Peter Chase, vice president of Library Connection and chairman of a state intellectual freedom committee. Chase -- "John Doe 1" in his affidavit -- advised Christian to call the ACLU. Reached by telephone at their homes, both men declined to be interviewed.

U.S. District Judge Janet C. Hall ruled in September that the FBI gag order violates Christian's, and Library Connection's, First Amendment rights. A three-judge panel heard oral argument on Wednesday in the government's appeal.

The central facts remain opaque, even to the judges, because the FBI is not obliged to describe what it is looking for, or why. During oral argument in open court on Aug. 31, Hall said one government explanation was so vague that "if I were to say it out loud, I would get quite a laugh here." After the government elaborated in a classified brief delivered for her eyes only, she wrote in her decision that it offered "nothing specific."

The Justice Department tried to conceal the existence of the first and only other known lawsuit against a national security letter, also brought by the ACLU's Jaffer and Ann Beeson. Government lawyers opposed its entry into the public docket of a New York federal judge. They have since tried to censor nearly all the contents of the exhibits and briefs. They asked the judge, for example, to black out every line of the affidavit that describes the delivery of the national security letter to a New York Internet company, including, "I am a Special Agent of the Federal Bureau of Investigation ('FBI')."

U.S. District Judge Victor Marrero, in a ruling that is under appeal, held that the law authorizing national security letters violates the First and Fourth Amendments.

Resistance to national security letters is rare. Most of them are served on large companies in highly regulated industries, with business interests that favor cooperation. The in-house lawyers who handle such cases, said Jim Dempsey, executive director of the Center for Democracy and Technology, "are often former prosecutors -- instinctively pro-government but also instinctively by-the-books." National security letters give them a shield against liability to their customers.

Kenneth M. Breen, a partner at the New York law firm Fulbright & Jaworski, held a seminar for corporate lawyers one recent evening to explain the "significant risks for the non-compliant" in government counterterrorism investigations. A former federal prosecutor, Breen said failure to provide the required information could create "the perception that your company didn't live up to its duty to fight terrorism" and could invite class-action lawsuits from the families of terrorism victims. In extreme cases, he said, a business could face criminal prosecution, "a 'death sentence' for certain kinds of companies."

The volume of government information demands, even so, has provoked a backlash. Several major business groups, including the National Association of Manufacturers and the U.S. Chamber of Commerce, complained in an Oct. 4 letter to senators that customer records can "too easily be obtained and disseminated" around the government. National security letters, they wrote, have begun to impose an "expensive and time-consuming burden" on business.

The House and Senate bills renewing the Patriot Act do not tighten privacy protections, but they offer a concession to business interests. In both bills, a judge may modify a national security letter if it imposes an "unreasonable" or "oppressive" burden on the company that is asked for information.

As national security letters have grown in number and importance, oversight has not kept up. In each house of Congress, jurisdiction is divided between the judiciary and intelligence committees. None of the four Republican chairmen agreed to be interviewed.

Roberts, the Senate intelligence chairman, said in a statement issued through his staff that "the committee is well aware of the intelligence value of the information that is lawfully collected under these national security letter authorities," which he described as "non-intrusive" and "crucial to tracking terrorist networks and detecting clandestine intelligence activities." Senators receive "valuable reporting by the FBI," he said, in "semi-annual reports [that] provide the committee with the information necessary to conduct effective oversight."

Roberts was referring to the Justice Department's classified statistics, which in fact have been delivered three times in four years. They include the following information: how many times the FBI issued national security letters; whether the letters sought financial, credit or communications records; and how many of the targets were "U.S. persons." The statistics omit one whole category of FBI national security letters and also do not count letters issued by the Defense Department and other agencies.

Committee members have occasionally asked to see a sampling of national security letters, a description of their fruits or examples of their contribution to a particular case. The Justice Department has not obliged.

In 2004, the conference report attached to the intelligence authorization bill asked the attorney general to "include in his next semiannual report" a description of "the scope of such letters" and the "process and standards for approving" them. More than a year has passed without a Justice Department reply.

"The committee chairman has the power to issue subpoenas" for information from the executive branch, said Rep. Zoe Lofgren (D-Calif.), a House Judiciary Committee member. "The minority has no power to compel, and . . . Republicans are not going to push for oversight of the Republicans. That's the story of this Congress."

In the executive branch, no FBI or Justice Department official audits the use of national security letters to assess whether they are appropriately targeted, lawfully applied or contribute important facts to an investigation.

Justice Department officials noted frequently this year that Inspector General Glenn A. Fine reports twice a year on abuses of the Patriot Act and has yet to substantiate any complaint. (One investigation is pending.) Fine advertises his role, but there is a puzzle built into the mandate. Under what scenario could a person protest a search of his personal records if he is never notified?

"We do rely upon complaints coming in," Fine said in House testimony in May. He added: "To the extent that people do not know of anything happening to them, there is an issue about whether they can complain. So, I think that's a legitimate question."

Asked more recently whether Fine's office has conducted an independent examination of national security letters, Deputy Inspector General Paul K. Martin said in an interview: "We have not

initiated a broad-based review that examines the use of specific provisions of the Patriot Act."

At the FBI, senior officials said the most important check on their power is that Congress is watching.

"People have to depend on their elected representatives to do the job of oversight they were elected to do," Caproni said. "And we think they do a fine job of it."

Researcher Julie Tate and research editor Lucy Shackelford contributed to this report.